OpenAmbient: a Pervasive Access Control Architecture

M. Anisetti, C.A. Ardagna, V. Bellandi,
E. Damiani, S. De Capitani di Vimercati, P. Samarati

1 Introduction

For a long time, lack of reliable security and privacy solutions has been considered to be a major hurdle toward the development of pervasive computing applications for critical domains such as secure workplace, healthcare and assisted living. Today, an advanced security infrastructure for context-aware and personalized authentication and authorization services in heterogeneous networks is gradually taking shape [4]. This infrastructure will enable large-scale mobility using a variety of mobile devices supporting authentication modules like SIMs [2, 3]. Also, it will rely on other emergent technologies such as video sensors supporting human posture and face interpretation [5, 8]. In such a scenario, fine-grained ambient information coming from monitoring and surveillance devices is used to enrich context representation underlying advanced access control and security policies. Our research approach [1] is aimed at a service-oriented architecture capable of preserving privacy and protecting resources, including personal user data. Specifically, we put forward the idea of integrating traditional access control models and mechanisms, based on the attributes of the requestor, with the emergent personalization and localization techniques to provide an ambient-aware, service-oriented access control model and language. In this paper we briefly present our Web Service-based architecture, named *OpenAmbient*, that incorporates a security language supporting ambient predicates.

2 Context Representation Issues

OpenAmbient takes into account several dynamic aspects that define the user context. Specifically, it captures the user's location, posture and expression, in addition to further profile information that makes up the overall context. Several formats for describing mobile users' profile data have been proposed such as the *Presence Information Data Format* (PIDF) [7]. However, some context representation issues cannot easily be dealt with through user profiles. In particular, considering security and privacy, two major classes of problems have to be addressed: *i)* user context information should only be provided to authorized entities, and *ii)* security and privacy of sensor data should be ensured. While several preliminary systems claim to control access to information coming from sensor networks, much work remains to be done to develop a complete access control mechanism relying on context data. A major challenge faced by OpenAmbient is managing intrinsic uncertainty and error held by location and video measurement. In principle, such information could be represented by extending device oriented profiling languages such as *Composite Capabilities /*

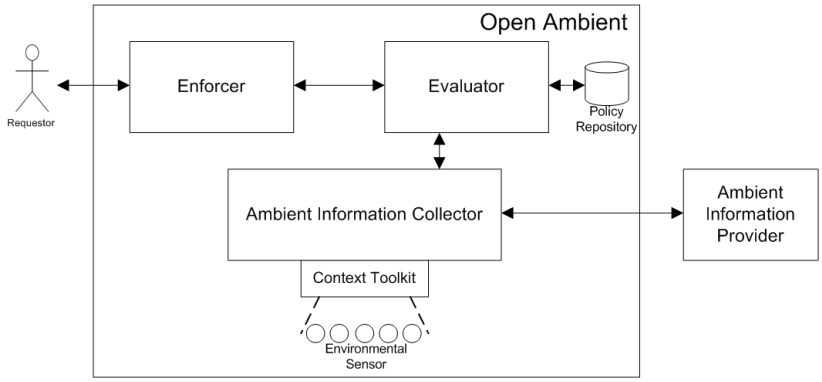

Figure 1: OpenAmbient Architecture

Preference Profile (CC/PP)[6]. OpenAmbient follows a different line of research, representing uncertainty underlying location and video sensor technologies in terms of a set of standard interfaces and semantically uniform *Service Level Agreement* (SLA) parameters negotiated between the involved parties to agree on the desired quality of service. The concept of Service Level Agreement (SLA) is used to designate the contract that the access control component, agree upon to manage the intrinsic uncertainty held by context information.

3 Open Ambient Architecture

The OpenAmbient architecture is composed by four major components (see Figure 1) joining concepts coming from traditional access control architectures and innovative ideas for the management of context information.

Enforcer. It represents the OpenAmbient external interface for the requestor. The Enforcer is the component responsible for the management and enforcement of the access control decision returned from the evaluator component. In particular, it grants to users access to a resource (e.g., an application service) only if a positive decision has been taken.

Evaluator. It represents the decision point. The evaluator is the component responsible for collecting the ambient-based policies and matching them against the requests submitted by the requestor. This component manages the intrinsic uncertainty of ambient-based predicates evaluation and it, finally, calculates the traditional *allow/deny* result.

Ambient Information Collector. It represents the component responsible for the interaction with the ambient data repository and/or technologies. It manages all the negotiation process that generates the SLA representing an agreement on the ambient information reliability. The required reliability can vary depending on different scenarios in which the OpenAmbient architecture acts. The ambient information collector, then, contains also a Context Toolkit that acts as an ambient information provider, when the ambient information resides in the OpenAmbient boundaries, managing the information retrieval process. In this case, the en-

vironment technologies and sensors, gathering context information, are directly managed by the OpenAmbient architecture.

Ambient Information Provider. It represents the component able to retrieve the requested ambient information. In particular, the provider could be logically internal to the OpenAmbient architecture (*Context Toolkit*) in the case in which the information are provided by technologies directly managed by it such as camera. Otherwise, as in the case of mobile technologies, the provider could be an external service (e.g. OpenWave Location Manager) that provides the requested data abstracting the underlying technologies.

OpenAmbient access control policies provide a high level of accountability and readability of assisted living and healthcare environments involving continuous monitoring and surveillance. From the functional point of view, OpenAmbient architecture faces the issues arising from the management of contextual information and uncertain measurements. In particular, it provides an infrastructure for the evaluation and enforcement of ambient-based policies. Then, OpenAmbient provides and implements different communication protocols managing the heterogeneity of the Ambient Information Provider. Finally, our architecture supplies a general-purpose negotiation protocol used by the involved parties to agree upon a SLA contract that will drive any further interaction. In the remainder of this paper we briefly elaborate on a running example illustrating security issues can occur in the domain of a secure workplace and how they can be addressed by the OpenAmbient approach. Then, we draw our conclusions.

Example 3.1 *The adoption of an ambient-aware access control model and architecture integrating emergent personalization and localization techniques is functional to the purpose of improving resource protection in high-critical environments, where malicious or inadvertent behaviors can cause a loss of critical information and/or moneys. As an example, we may consider a highly-critical work environment, such as an automated bank. This environment includes services like an automatic* deposit drop box*, where users drop their deposits to be later collected by bank employees. Each drop box is protected by a timer that allows access only at pre-determined times. Also, access is granted only if the employee has been authenticated upon entering the box area by means of a key/badge. In this critical environment, however, a malicious authorized user could steal the badge of an authorized employee to access the drop box without the fulfillment of the requested conditions. Ambient-based conditions can prevent this type of attack, making the (ubiquitous) access control infrastructure more secure and reliable. Suppose that, the security administrator defines a policy allowing the access to the drop box only if the authorized user is located inside the area where the box is according to reliable positioning techniques such as mobile phone positioning, RFID, GPS and so forth. In addition, the security administrator requires that the user must be identified by the surveillance cameras as a member of a pool of authorized users, by means of face identification techniques. Finally, the administrator requires the user not to be alone in the area where the box is located. The syntax is as follows*[1].

`any` WITH ***User***.category = `trustedUsers` CAN access ON *bankDepositBox* IF
`density`*(bankDepositArea,1,unbounded)* AND `faceIdentification`*(**User**,trustedPool)* AND
`inArea`*(**User**,bankDepositArea)*

[1]The language syntax has been defined in the context of European Project PRIME (Privacy and Identity Management for Europe, http://www.prime-project.eu.org/)

4 Conclusion

Ubiquitous access control allows for writing and enforcing ambient security policies improving the overall security of a critical workplace or an assisted living environment. The adoption of ambient-based conditions as a part of a sound access control model and architecture provides a set of functionalities substantially improving robustness of ubiquitous access control.

References

[1] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Supporting location-based conditions in access control policies. In *Proc. of the ACM Symposium on InformAtion, Computer and Communications Security(ASIACCS'06)*, Taipei, Taiwan, March 2006.

[2] P. Bhal and V. N. Padmanabhan. Radar: An in-building rf-based user location and tracking system. *IEEE INFOCOM*, 2000.

[3] A. Corallo, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, G. Elia, and P. Samarati. Security, Privacy, and Trust in Mobile Systems. In *Mobile and Wireless Systems beyond 3G: managing new business opportunities, Idea Group Inc.*, 2005.

[4] M.J. Covington, W. Long, S. Srinivasan, A.K. Dey, and G.D. Abowd M. Ahamad. Securing context-aware applications using environment roles. In *SACMAT 2001*, 2001.

[5] E. Damiani, M. Anisetti, V.Bellandi, and F. Beverina. Facial identification problem: A tracking based approach. In *Proc. of the IEEE International Symposium on Signal-Image Technology and InternetBased Systems (IEEE SITIS'05)*, Yaoundé, Cameroon, November 2005.

[6] Franklin R. et al. Composite capability/preference profiles (cc/pp): Structure. *W3C Working Draft*, 2000.

[7] Sugano H. et al. Presence information data format (pidf). *Network Working Group, IETF, Internet Draft*, 2003.

[8] M.J. Turk and A. Pentland. Eigenfaces for recognition. In *IFIP Working Con- ference on Engineering for Human-Computer Interaction*, volume 3, pages 71–86, 1991.